



BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

REC'D 01 SEP 2003

WIPO

PCT

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 02 MAI 2003

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

**PRIORITY
DOCUMENT**
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1 (a) OR (b)

Martine PLANCHE

BEST AVAILABLE COPY

INSTITUT
NATIONAL DE
PROPRIÉTÉ
INDUSTRIELLE

SIEGE
26 bis, rue de Saint Petersburg
75800 PARIS cedex 08
Téléphone : 33 (0)1 53 04 53 04
Télécopie : 33 (0)1 53 04 45 23
www.inpi.fr



26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



REQUÊTE EN DÉLIVRANCE page 1/2

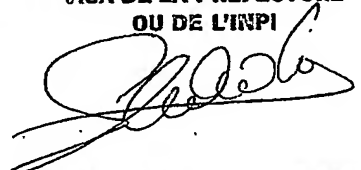


Cet imprimé est à remplir lisiblement à l'encre noire

08 540 0 W / 010501

REMISE DES PIÈCES DATE 24 JUIL 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0209361 NATIONAL ATTRIBUÉ PAR L'INPI DATE DE DÉPÔT ATTRIBUÉE PAR L'INPI 24 JUIL. 2002		51 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE THOMSON multimedia Attn. : M. Thierry KERBER 46, quai Alphonse le Gallo 92648 Boulogne Billancourt cedex FRANCE	
Vos références pour ce dossier (facultatif) PF020092			
Confirmation d'un dépôt par télécopie		<input type="checkbox"/> N° attribué par l'INPI à la télécopie	
2 NATURE DE LA DEMANDE		Cochez l'une des 4 cases suivantes	
Demande de brevet		<input checked="" type="checkbox"/>	
Demande de certificat d'utilité		<input type="checkbox"/>	
Demande divisionnaire		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date _____	
ou demande de certificat d'utilité initiale		N° _____ Date _____	
Transformation d'une demande de brevet européen		<input type="checkbox"/>	
Demande de brevet initiale		N° _____ Date _____	
3 TITRE DE L'INVENTION (200 caractères ou espaces maximum) Méthode pour distribuer des portions cryptées d'un programme audiovisuel			
4 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE FRANÇAISE		Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ Date _____ Pays ou organisation _____ N° _____ <input type="checkbox"/> S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»	
5 DEMANDEUR (Cochez l'une des 2 cases)		<input checked="" type="checkbox"/> Personne morale <input type="checkbox"/> Personne physique	
Nom ou dénomination sociale		THOMSON Licensing S.A.	
Prénoms			
Forme juridique			
N° SIREN		3 8 3 4 6 1 1 9 1	
Code APE-NAF		3 2 2 A	
Domicile ou siège	Rue	46, quai Alphonse le Gallo	
	Code postal et ville	9 2 1 0 0 Boulogne Billancourt	
	Pays	France	
Nationalité		Française	
N° de téléphone (facultatif)		+ 33 1 41 86 69 55 N° de télécopie (facultatif) + 33 1 41 86 56 33	
Adresse électronique (facultatif)		kerbert@thmulti.com	
<input type="checkbox"/> S'il y a plus d'un demandeur, cochez la case et utilisez l'imprimé «Suite»			

Remplir impérativement la 2^{ème} page

REMISE DES PIÈCES DATE 24 JUIL 2002 LIEU 75 INPI PARIS N° D'ENREGISTREMENT 0209361 NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI	DB 540 G W / 010801
Vos références pour ce dossier : (facultatif)		PF020092	
6 MANDATAIRE (s'il y a lieu)		Les inventeurs sont nécessairement des personnes physiques	
Nom		KERBER	
Prénom		Thierry	
Cabinet ou Société		THOMSON multimedia	
N° de pouvoir permanent et/ou de lien contractuel		9016	
Adresse	Rue	46, quai Alphonse le Gallo	
	Code postal et ville	91206 1418 Boulogne Billancourt cedex	
	Pays	FRANCE	
N° de téléphone (facultatif)		+ 33 1 41 86 69 55	
N° de télécopie (facultatif)		+ 33 1 41 86 56 33	
Adresse électronique (facultatif)		kerbert@thmulti.com	
7 INVENTEUR (S)		Les inventeurs sont nécessairement des personnes physiques	
Les demandeurs et les inventeurs sont les mêmes personnes		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non : Dans ce cas remplir le formulaire de Désignation d'Inventeur(s)	
8 RAPPORT DE RECHERCHE		Uniquement pour une demande de brevet (y compris division et transformation)	
Établissement immédiat ou établissement différé		<input checked="" type="checkbox"/> Oui <input type="checkbox"/> Non	
Paiement échelonné de la redevance (en deux versements)		Uniquement pour les personnes physiques effectuant elles-mêmes leur propre dépôt <input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non	
9 RÉDUCTION DU TAUX DES REDEVANCES		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Obtenue antérieurement à ce dépôt pour cette invention (joindre une copie de la décision d'admission à l'assistance gratuite ou indiquer sa référence) : AG <input type="text"/>	
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		<input type="text"/>	
10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (Nom et qualité du signataire) KERBER Thierry Mandataire		VISA DE LA PRÉFECTURE OU DE L'INPI 	

L'invention concerne une méthode pour distribuer des portions cryptées d'un programme audiovisuel à des terminaux utilisateurs, en particulier des décodeurs pour récepteur de télévision, dans laquelle les portions successives du programme sont cryptées à l'aide de clés différentes avant d'être distribuées
5 aux terminaux utilisateurs.

Dans la présente demande, on désigne par « programme audiovisuel » tout programme pouvant être audio, vidéo, ou à la fois audio et vidéo. Un tel programme peut notamment consister en un programme multimédia de type MPEG 4, pouvant contenir par exemple plusieurs séquences vidéo et/ou audio,
10 des données tridimensionnelles, des graphiques bidimensionnels et/ou des scripts d'animation associés.

Une méthode de distribution de portions cryptées est connue du document de brevet EP-1075108. Dans cette méthode, une ou plusieurs valeurs de germe sont communiquées sélectivement aux terminaux utilisateurs pour qu'ils puissent
15 régénérer localement un ensemble limité de clés de décryptage permettant de décrypter un nombre limité correspondant de portions cryptées du programme. La communication des valeurs de germe fait l'objet d'une facturation à l'utilisateur dont le montant peut varier en fonction de l'étendue du décryptage. Il peut s'agir par exemple d'une facturation à la séance ou par abonnement. Un
20 système de facturation par abonnement s'avère complexe à mettre en place au niveau d'un centre audiovisuel qui fournit les programmes cryptés. Par ailleurs, la facturation à la séance augmente globalement le coût d'utilisation du service audiovisuel pour l'utilisateur dans le cas où il ne profite que d'une fraction du programme.

25 Le but de l'invention est de proposer une méthode pour distribuer des portions cryptées d'un programme audio et/ou vidéo qui rend possible une facturation plus simple et plus fine du service tout en offrant une sécurité contre le piratage.

La méthode selon l'invention est caractérisée en ce qu'elle consiste, sur
30 initiation, depuis un terminal utilisateur, d'une communication téléphonique avec un centre d'appel, à transmettre en séquence depuis ce centre d'appel et pendant la communication téléphonique les clés au terminal utilisateur et ceci de

manière synchronisée avec la distribution des portions successives cryptées du programme. Bien entendu, la distribution des portions cryptées successives du programme peut être réalisée par diffusion sur câble, par satellite ou par faisceau hertzien. Le centre d'appel est de préférence un centre de réception d'appels
5 téléphoniques d'un opérateur téléphonique dans lequel il existe des moyens pour mesurer à chaque appel d'un terminal utilisateur, le temps de la communication téléphonique avec celui-ci de sorte qu'à partir de cette information, une facture appropriée peut être générée facilement pour l'utilisateur correspondant. On comprend que tant que la communication téléphonique est établie entre le centre
10 d'appel et un terminal utilisateur, un décryptage des portions courantes du programme est rendu possible localement dans le terminal utilisateur. Mais au terme de la communication téléphonique, les portions cryptées courantes du programme ne sont plus décryptées puisque les clés n'arrivent plus dans le terminal utilisateur. La durée de réception en clair du programme correspond
15 donc globalement à la durée de la communication téléphonique de sorte que l'utilisateur ne paie que pour la durée effective durant laquelle il profite du service audiovisuel. La méthode selon l'invention présente encore avantageusement les particularités suivantes:

- la communication téléphonique exploite un protocole Internet ;
- 20 - des codes temporels de synchronisation sont transmis en correspondance avec les clés successives pendant la communication téléphonique.

L'invention s'étend à un décodeur pour récepteur de programmes audio et/ou vidéo dans lequel des portions successives d'un programme sont
25 décryptées à l'aide d'une succession de clés différentes, caractérisé en ce qu'il est agencé pour se connecter, par l'intermédiaire d'une interface de communication téléphonique, à un centre d'appel et pour récupérer en séquence les clés successives pendant la communication avec le centre d'appel et ceci de manière synchronisée avec le décryptage des portions successives du
30 programme.

Selon des particularités préférées de ce décodeur:

- l'interface de communication téléphonique est un modem téléphonique notamment du type modem ADSL qui exploite un protocole Internet.

L'invention s'étend encore à une routine de décryptage adaptée pour être chargée dans la mémoire d'un décodeur pour récepteur de programmes audio et/ou vidéo disposant d'une interface de communication téléphonique.

La méthode, le décodeur et la routine selon l'invention sont décrits ci-après plus en détail et illustrés à travers la figure unique qui représente schématiquement un système de distribution de programmes vidéo et/ou audio payants.

On a représenté sur la figure à titre d'exemple non limitatif seulement deux terminaux utilisateurs T1,T2 comprenant chacun un récepteur R1,R2 de programmes audio et/ou vidéo, un décodeur D1,D2 ainsi qu'une interface de communication M1,M2 du type modem téléphonique.

Les récepteurs R1,R2 sont ici des récepteurs de télévision. Les interfaces de communication M1,M2 pourraient faire partie intégrante respectivement des décodeurs D1,D2 qui peuvent être des décodeurs du type "set top box".

Chaque décodeur D1,D2 est apte à recevoir sur un canal d'entrée C1,C2 des portions cryptées successives d'un programme audio et/ou vidéo. Ces portions de programme sont des trames numériques.

Les portions cryptées du programme sont distribuées ici aux terminaux utilisateurs T1,T2 par le canal hertzien 1 depuis une antenne de diffusion 2 qui est reliée à un centre audiovisuel 3 fournisseur du programme. Dans le centre audiovisuel 3, les portions successives du programme sont cryptées en utilisant une succession de clés de cryptage différentes de façon à limiter les possibilités de piratage. La clé de cryptage utilisée pour crypter les portions successives du programme est changée à la fin de chaque séquence de n portions successives, la valeur de n étant ajustée pour avoir une clé de cryptage différente par exemple toutes les 30 secondes de présentation du programme à l'écran.

On connaît l'usage des codes temporels dans les flux audiovisuels numériques: DTS (Decoding Time Stamp); PTS (Presentation Time Stamp) et PCR (Program Clock Reference) dans les flux MPEG2-TS. Ces codes temporels sont insérés dans chaque portion cryptée du programme et permettent de

synchroniser le décodeur D1,D2 sur l'horloge de l'émetteur 3 du programme audiovisuel.

Selon un aspect de l'invention, on associe lors du cryptage dans le centre audiovisuel 3, des codes temporels du type DTS aux différentes clés de cryptage. Cette association servira lors du décryptage des portions du programme dans un décodeur à empêcher le décryptage d'une portion du programme si le code temporel associé à la clé de décryptage fournie pour cette portion du programme n'est pas synchronisé avec le code temporel DTS récupéré dans cette portion du programme.

10 La référence 4 sur la figure indique un centre d'appel téléphonique qui reçoit en séquence du centre audiovisuel 3 la succession de clés de cryptage et ceci de manière synchronisée avec la diffusion des portions successives du programme par l'antenne 2 et donc avec la réception en séquence de ces portions du programme par les terminaux utilisateurs T1,T2.

15 Pour que le programme soit présenté en clair au niveau du récepteur R1,R2 d'un terminal utilisateur T1,T2, l'utilisateur actionne son décodeur D1,D2, par exemple par le biais d'une commande manuelle F1,F2 ou d'une télécommande qui force le décodeur à initier une communication téléphonique avec le centre d'appel 4 par l'intermédiaire d'une interface de communication
20 M1,M2 du type modem. Le numéro d'appel du centre d'appel pourra être préenregistré dans le décodeur pour rendre automatique l'ouverture de la communication téléphonique. Pendant la communication téléphonique, le décodeur D1,D2 pourra être identifié par le centre d'appel 4 et à l'issue de l'identification, le centre d'appel 4 transmet en séquence par la voie téléphonique
25 vers le terminal utilisateur T1,T2 les clés successives courantes servant au décryptage des portions courantes du programme que reçoit en parallèle le décodeur D1,D2. La transmission en séquence par le centre d'appel 4 de ces clés associées chacune avec un code temporel se fait de manière synchronisée avec la diffusion des portions du programme par l'antenne 2. Sur la figure,
30 "x,y,z,..." représente les clés de décryptage successives et "t1,t2,t3,..." représente les codes temporels associés aux clés de décryptage.

Dans chaque décodeur D1,D2, le processus de décryptage s'organise de telle manière que les clés successives avec les codes temporels associés récupérés par l'intermédiaire de l'interface de communication M1,M2 sont contrôlés par comparaison avec les codes temporels DTS se trouvant dans les portions cryptées du programme que reçoit le décodeur. En d'autres termes, une
5 clé associée à un code temporel t1 sera rejetée si la portion du programme reçue parallèlement à la récupération de cette clé contient un code temporel DTS antérieur à t1. Cette portion de programme ne sera donc pas décryptée dans le décodeur. En pratique, les clés successives avec les codes temporels respectifs
10 sont récupérés dans le terminal utilisateur avec une légère avance par rapport aux portions de programme correspondantes et un stockage temporaire des clés doit donc être organisé dans le décodeur pour permettre le décryptage lors de la réception de la portion courante de programme. Quand une clé avec un code temporel t1 est récupérée par le décodeur, elle est stockée dans la mémoire
15 temporaire du décodeur si le code temporel DTS de la portion courante du programme est antérieur au code temporel t1 associé à la clé. Dans le cas contraire, la clé est rejetée et n'est donc pas enregistrée dans la mémoire temporaire du décodeur. Lors du décryptage d'une portion courante du programme, la clé nécessaire à ce décryptage devra être présente dans la
20 mémoire temporaire du décodeur.

Le processus de décryptage ci-dessus peut être mis en œuvre par une routine chargée en mémoire dans un décodeur classique programmable équipé d'une interface de communication téléphonique.

L'interface de communication sera de préférence un modem du type
25 ADSL qui exploitera avantageusement un protocole de communication Internet pour permettre des communications multiples sur la même ligne téléphonique.

REVENDICATIONS

1/ Méthode pour distribuer des portions cryptées d'un programme audiovisuel à des terminaux utilisateurs (T1,T2) dans laquelle les portions
5 successives du programme sont cryptées à l'aide de clés différentes, caractérisée en ce qu'elle consiste, sur initiation, depuis un terminal utilisateur, d'une communication téléphonique avec un centre d'appel (4), à transmettre en séquence depuis ce centre d'appel et pendant la communication téléphonique les clés au terminal utilisateur et ceci de manière synchronisée avec la
10 distribution des portions cryptées successives du programme.

2/ Méthode selon la revendication 1, dans laquelle la communication téléphonique exploite un protocole Internet.

15 3/ Méthode selon l'une des revendications 1 à 2, dans laquelle des codes temporels sont transmis avec les clés au terminal utilisateur.

4/ Méthode selon l'une des revendications 1 à 3, dans laquelle au terme de la communication téléphonique avec un terminal utilisateur, une durée de
20 communication téléphonique est déterminée dans le centre d'appel pour l'établissement d'une facture correspondant à la réception du programme par le terminal utilisateur.

5/ Méthode selon l'une des revendications 1 à 4, dans laquelle le centre
25 d'appel est un centre de réception d'appels téléphoniques d'un opérateur téléphonique.

6/ Décodeur (D1,D2) pour récepteur de programmes audiovisuels dans lequel des portions successives d'un programme sont décryptées à l'aide d'une
30 succession de clés différentes, caractérisé en ce qu'il est agencé pour se connecter, par l'intermédiaire d'une interface de communication téléphonique (M1,M2), à un centre d'appel (4) et pour récupérer en séquence les clés

successives pendant la communication avec le centre d'appel et ceci de manière synchronisée avec le décryptage des portions successives du programme.

7/ Décodeur selon la revendication 6, agencé pour récupérer du centre
5 d'appel des codes temporels en association avec les clés

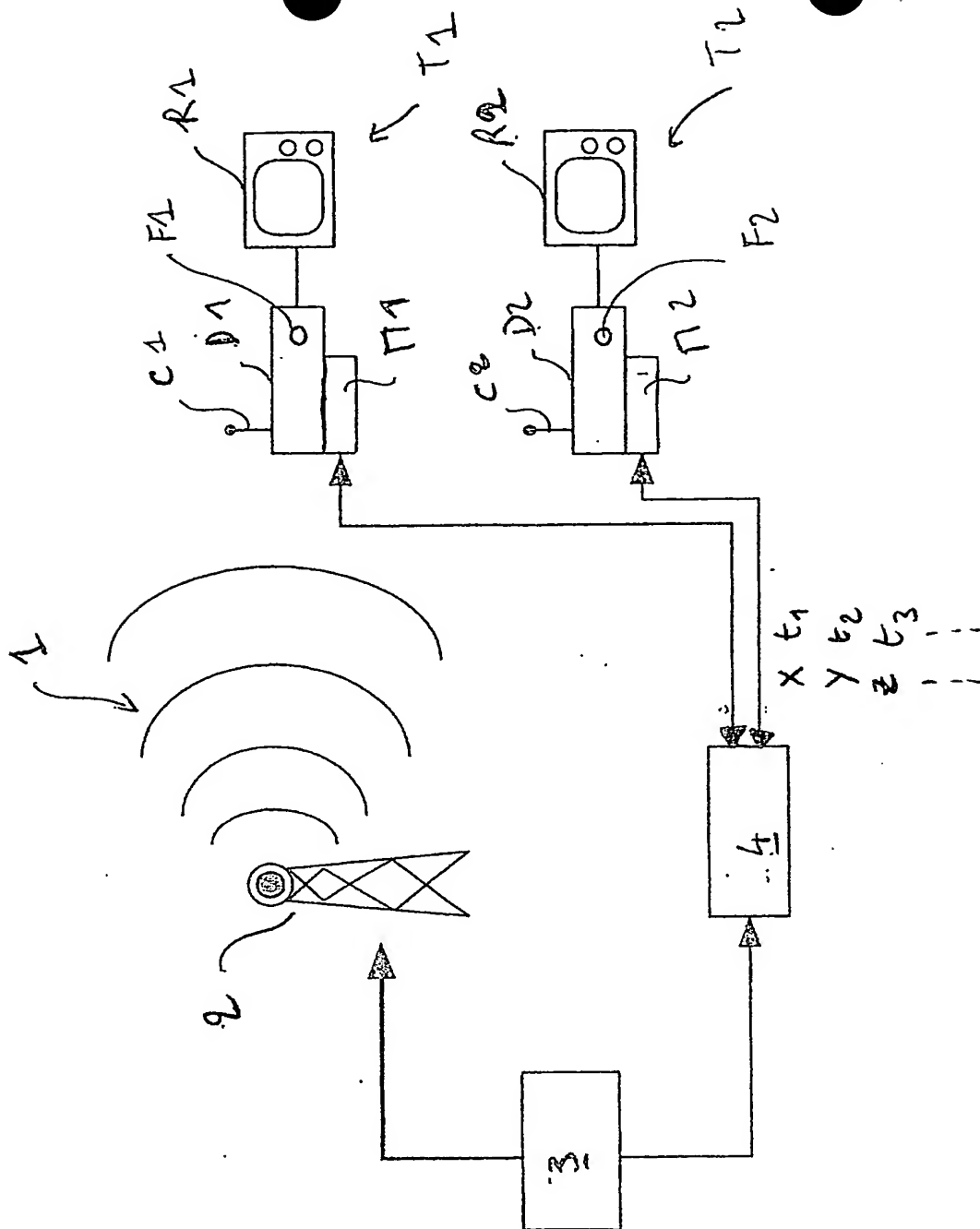
8/ Décodeur selon la revendication 7, dans lequel l'interface de communication est un modem téléphonique.

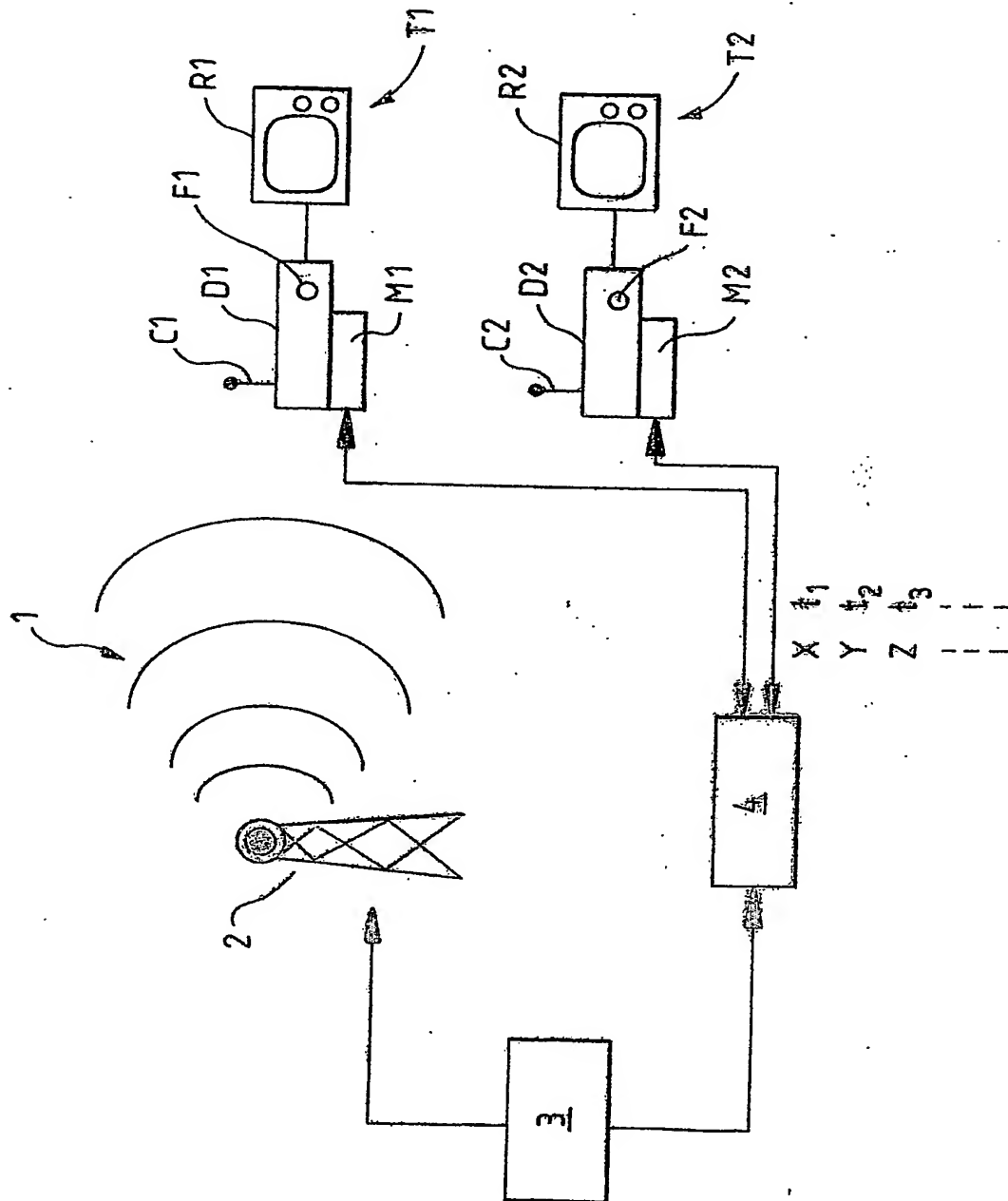
10 9/ Décodeur selon la revendication 8, dans lequel l'interface de communication exploite un protocole Internet.

10/ Décodeur selon la revendication 9, dans lequel l'interface de communication est un modem ADSL.
15

11/ Routine de décryptage pour décrypter des portions successives d'un programme audiovisuel à l'aide d'une succession de clés différentes, caractérisée en ce qu'elle est agencée pour établir une communication téléphonique avec un centre d'appel (4) ayant un numéro d'appel prédéfini et en
20 ce qu'elle est agencée pour récupérer du centre d'appel les clés successives pendant la communication téléphonique et ceci de manière synchronisée avec le décryptage des portions successives du programme.

12/ Méthode pour décoder un programme audiovisuel selon laquelle des
25 portions successives du programme sont décryptées à l'aide d'une succession de clés différentes, caractérisée en ce qu'elle consiste à se connecter, par l'intermédiaire d'une interface de communication téléphonique (M1,M2), à un centre d'appel (4) pour récupérer en séquence les clés successives pendant la communication avec le centre d'appel et ceci de manière synchronisée avec le
30 décryptage des portions successives du programme.







BREVET D'INVENTION
CERTIFICAT D'UTILITE

Code de la propriété intellectuelle - Livre VI


N° 11235*03

DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54


DÉSIGNATION D'INVENTEUR(S) Page N° 1.. / 1..

(À fournir dans le cas où les demandeurs et les inventeurs ne sont pas les mêmes personnes)



Cet imprimé est à remplir lisiblement à l'encre noire

DB 113 C W / 270601

Vos références pour ce dossier (facultatif)		PF020092
N° D'ENREGISTREMENT NATIONAL		0209361
TITRE DE L'INVENTION (200 caractères ou espaces maximum) Méthode pour distribuer des portions cryptées d'un programme audiovisuel		
LE(S) DEMANDEUR(S) : THOMSON Licensing S.A.		
DESIGNE(NT) EN TANT QU'INVENTEUR(S) :		
1 Nom		BORDES
Prénoms		Philippe
Adresse	Rue	21, route de Nantes
	Code postal et ville	3 5 1 3 1 PONT-PEAN
Société d'appartenance (facultatif)		
2 Nom		GUILLOT
Prénoms		Philippe
Adresse	Rue	60, rue de Châteaubriant
	Code postal et ville	3 5 7 7 0 VERN SUR SEICHE
Société d'appartenance (facultatif)		
3 Nom		FRANCOIS
Prénoms		Edouard
Adresse	Rue	18, allée du Locar
	Code postal et ville	3 5 8 9 0 BOURG DES COMPTES
Société d'appartenance (facultatif)		
S'il y a plus de trois inventeurs, utilisez plusieurs formulaires. Indiquez en haut à droite le N° de la page suivi du nombre de pages.		
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire) 22/07/2002  KERBER Thierry Mandataire		

La loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés s'applique aux réponses faites à ce formulaire.
Elle garantit un droit d'accès et de rectification pour les données vous concernant auprès de l'INPI.

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

☐ BLACK BORDERS

☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES

☒ FADED TEXT OR DRAWING

☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING

☐ SKEWED/SLANTED IMAGES

☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS

☐ GRAY SCALE DOCUMENTS

☐ LINES OR MARKS ON ORIGINAL DOCUMENT

☒ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY

☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.